Log4J Vulnerabilities - SonicWall Resolutions (Updated to 20 Dec 2021)

The information provided below is referred from https://www.sonicwall.com/support/notices/security-notice-apache-log4j-remote-code-execution-rce-log4shell-vulnerability-cve-2021-44228/211214102517010/ and https://blog.sonicwall.com/en-us/2021/12/how-sonicwall-ztna-protects-against-log4j-log4shell /.

- **CVE Number**

  2021-44228

- **Discovery Date**

  No information

- **Threat Level**

Critical

- **Response to Log4j**

The Apache Log4j project disclosed CVE-2021-44228, which is a critical (CVSS 10.0) remote code execution (RCE) vulnerability affecting Apache Log4j2<= 2.14.1. A security patch(Log4j 2.15.0) was released on December 10, 2021, and another patch (Log4j 2.16.0) released on December 14, 2021.

- **Affected SonicWall Products**

SonicWall has the following products that impacted by the log4j Vulnerabilities.

1. Email Security
2. NSM

- **SonicWall Protection**

SonicWall Cloud Edge is built on zero-trust architecture that enables access and network connectivity to internal and external resources. By combining Cloud Edge Zero Trust Network Architecture (ZTNA) and tightly defined policies, admins can ensure servers are not publicly exposed to the internet, but only to users who meet certain criteria and are allowed to pass through network firewall or Stateful FWaaS.

Using ZTNA and SDP architecture to protect and hide all of the underlying services from public access, we can mitigate the Log4Shell vulnerability by only passing activity logs within the internal network. SonicWall Cloud Edge ZTNA by default will not allow them to be sent outside the local network over a public internet connection.

SonicWall Cloud Edge significantly reduces the attack surface and potential damage to the internal network by allowing admins to precisely control and limit any traffic generated from inside or outside the network. By segmenting your cloud, on-prem or hybrid network with ZTNA, you can also contain the spread of malicious code or activity within your defined network perimeter.